RSAC 2025 Conference

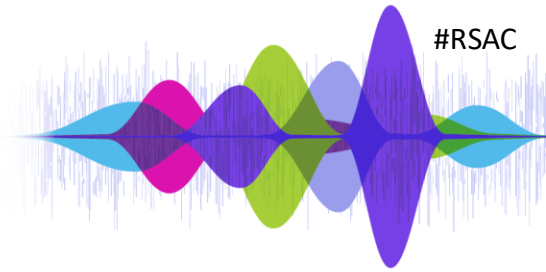
Many Voices. One Community.

SESSION ID: CSO-M06

Reporting Lines Matter: The 2025 CISO's Place In the Org Chart

Todd Fitzgerald

CISO, Cybersecurity and Privacy Leadership Author and Advisor
CISO SPOTLIGHT, LLC
www.linkedin.com/in/toddfitzgerald



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Todd Fitzgerald

Cybersecurity and Privacy Leadership Author, Podcaster, Advisor

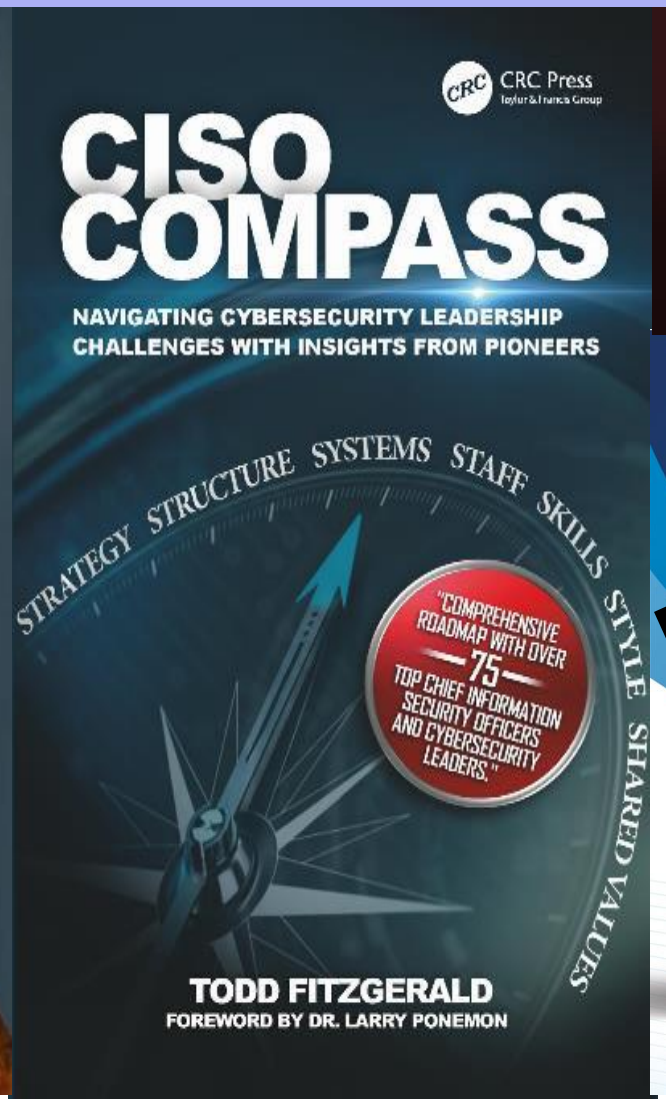
CISO SPOTLIGHT, LLC

Trusted Cybersecurity and Privacy Training

RSAC 2025 Conference

Todd Fitzgerald

Cybersecurity and Privacy Leadership Author, Podcaster, Advisor


CRC Press
Taylor & Francis Group
CISO COMPASS
NAVIGATING CYBERSECURITY LEADERSHIP CHALLENGES WITH INSIGHTS FROM PIONEERS
STRATEGY STRUCTURE SYSTEMS STAFF SKILLS STYLE SHARED VALUES
"COMPREHENSIVE ROADMAP WITH OVER 75 TOP CHIEF INFORMATION SECURITY OFFICERS AND CYBERSECURITY LEADERS."
TODD FITZGERALD
FOREWORD BY DR. LARRY PONEMON

CISO SPOTLIGHT, LLC

Trusted Cybersecurity and Privacy Training

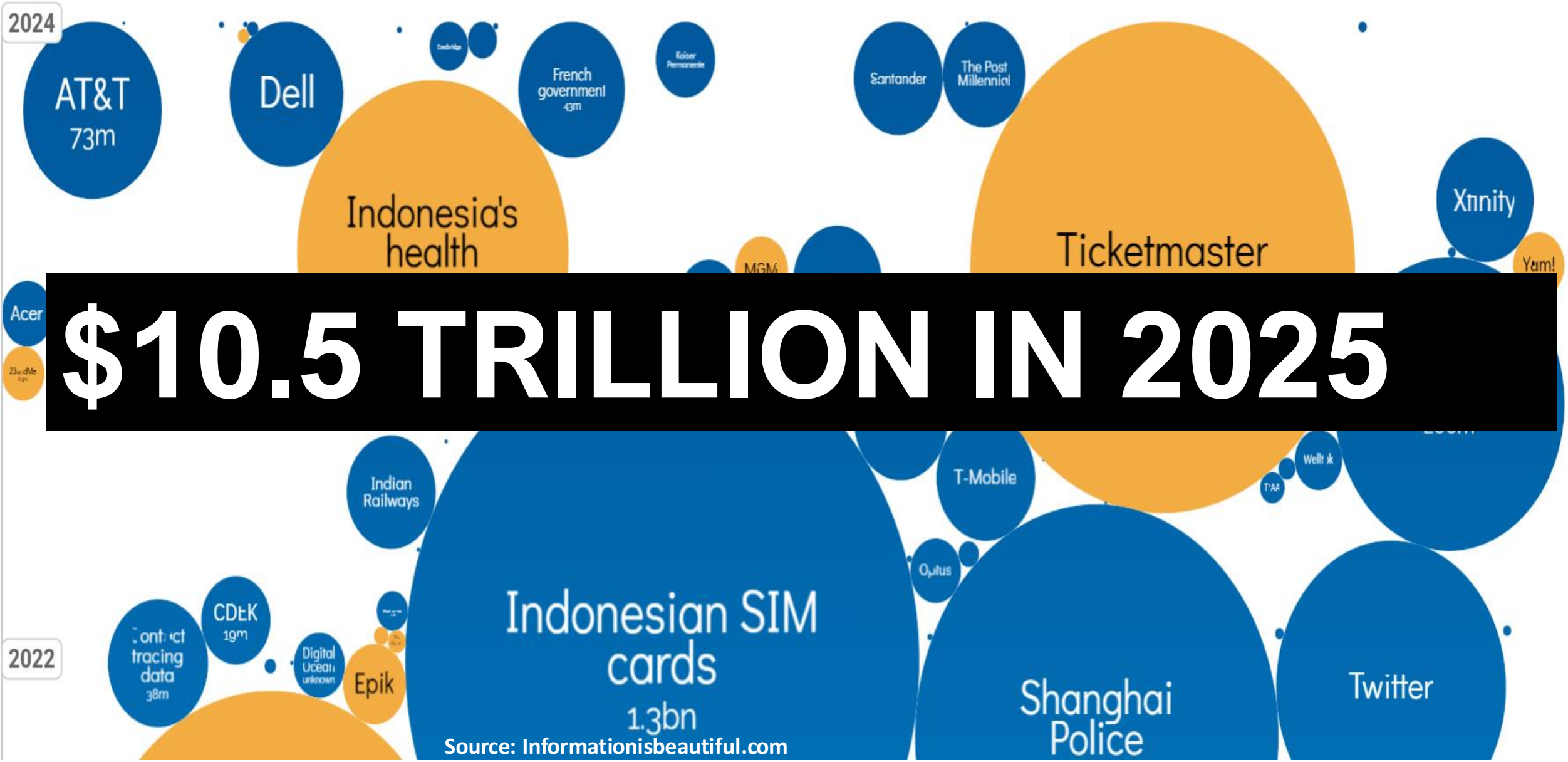
RSAC 2025 Conference

RSAC | 2025 Conference

TODAY'S AGENDA

1. The CISO Evolution and 6 CISO Key Focus Areas
2. CISO Reporting Relationships PROs and CONS
3. Where CISOs Report Today – Surveys Say
4. Board Reporting/Final Thoughts

Many Voices.
One Community.



Source: Informationisbeautiful.com

SOLUTION: We Recruit a

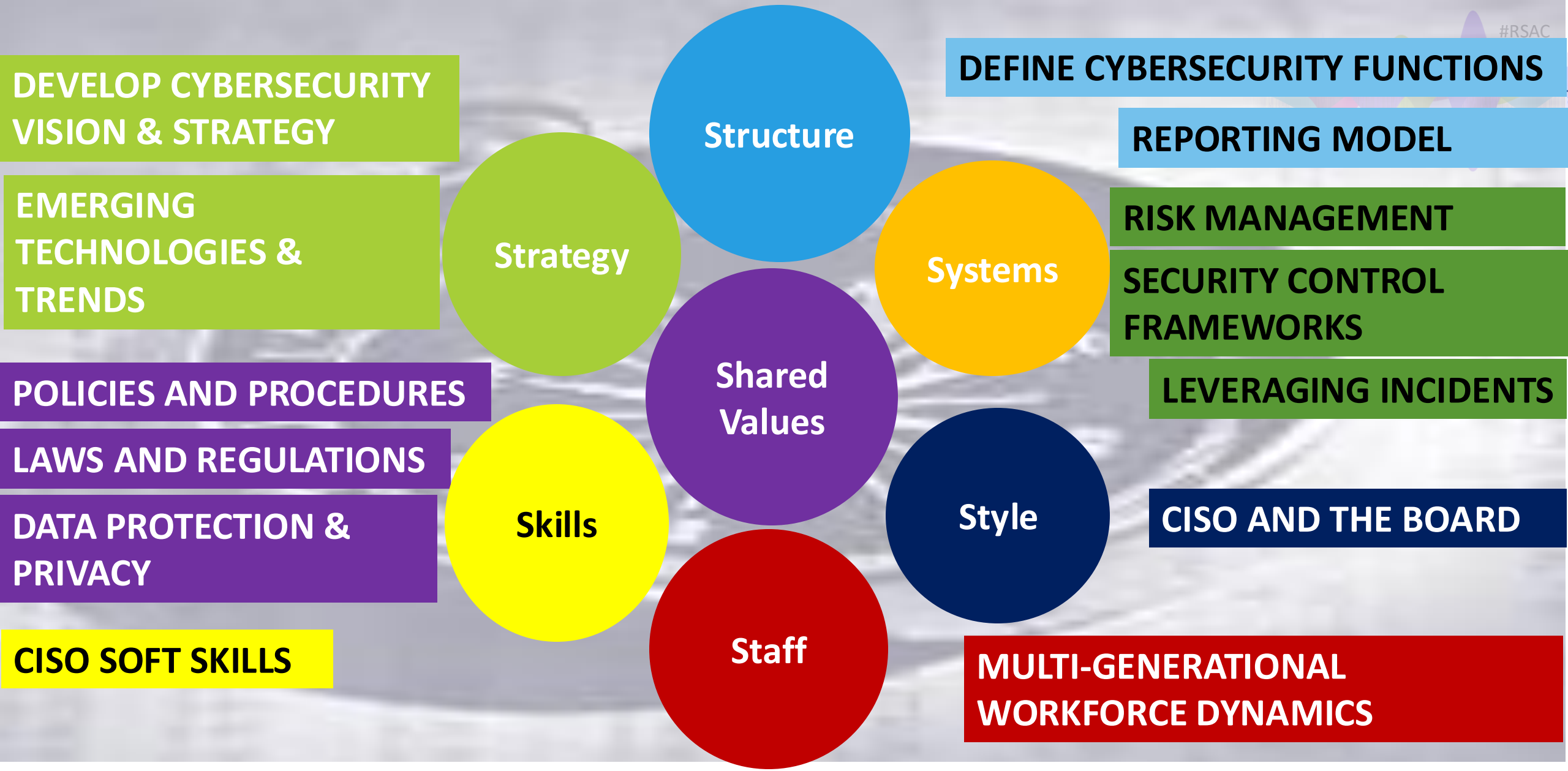
CISO

Chief Information Security Officer

7,523 CISOS IN USA
GLOBAL CISOS=32,000
69,420 CIOs
90% Do Not Have a CISO

RSAC 2025 Conference

1. The 30 Year CISO Evolution Created 6 Focus Areas

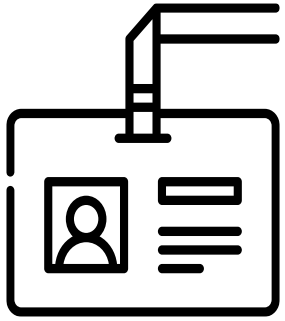


Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

6 Key CISO FOCUS Areas

Question 1: What Is YOUR CISO Primary Focus Area?

CISO EVOLUTION 1995-2027



1990s-2000

1 Security= Logon & Password FIRST CISO

2000-2004

2 Regulatory Compliance Era CISOs Hired

2004-2008

3 Risk-Oriented CISO Emerges

2008-2016

4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

2016-2022

5 The Privacy and Data-Aware CISO

2022-2027+

6 The Integrated Business Resilient CISO

Source: Adapted From T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications), New 6 Stage Model Updated in K. Engemann, J. Witty, Cybersecurity Risk Management (2024, De Gruyter)

1990s-2000

1. THE TECHNICAL CISO

THE FIRST SECURITY LEADERS

(Video Automatically Plays On This Slide)

2000-2004

2. THE COMPLIANCE CISO

STANDARDS

COMPLIANCE

=SECURITY

In the Wake of a
Shipping Mishap off
the Coast of Australia

(Video Automatically Plays On This Slide)

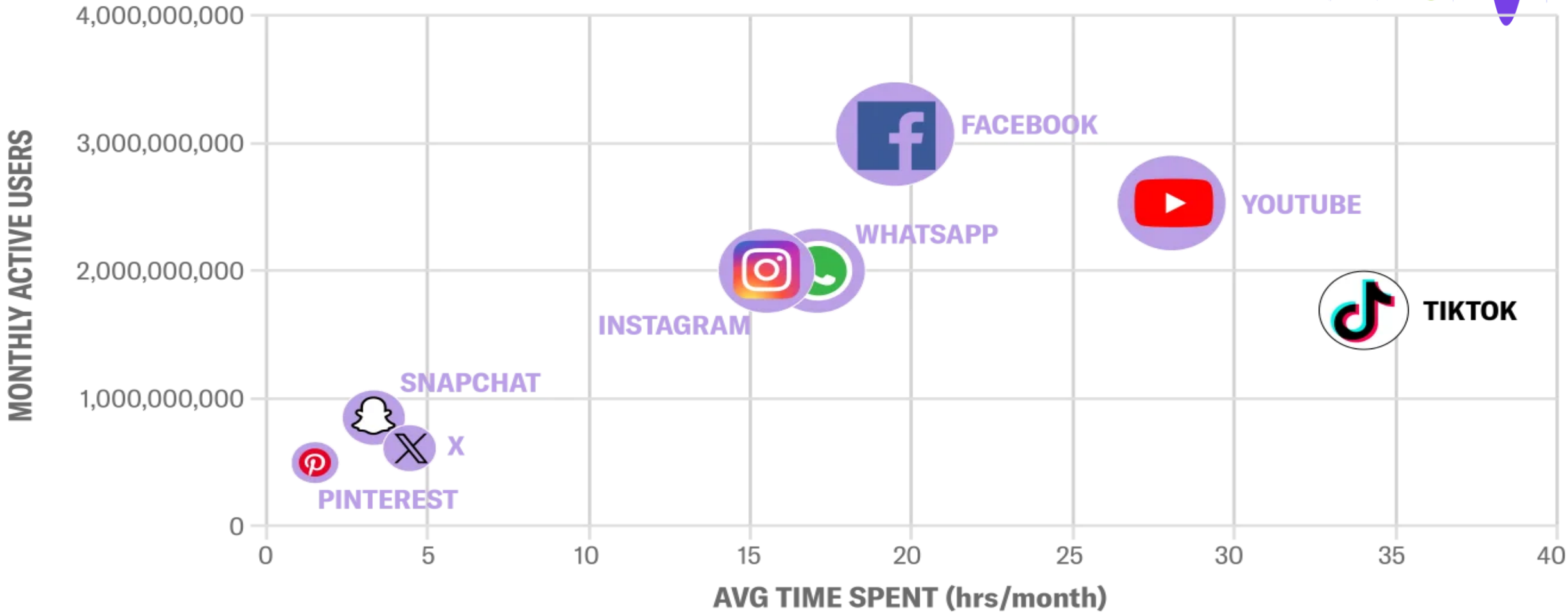
2004-2008

3.THE RISK MANAGEMENT CISO

2008-2016

4. THE THREAT-AWARE CYBERSECURITY-SOCIALLY-MOBILE-CLOUD CISO

COURTESY: AMAZON



SOURCE: DATAREPORTAL, STATISTA

2016-2022

5. THE PRIVACY AND DATA-AWARE CISO

GDPR
General Data Protection Regulation
Comliance
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse malesuada aliquam lectus et mollis. Aliquam tincidunt diam a sapien pharetra ve-hicula. Sed cursus augue quis porttitor molestie.
Privacy
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse malesuada aliquam lectus et mollis. Aliquam tincidunt diam a sapien pharetra ve-hicula. Sed cursus augue quis porttitor molestie.
Personal data
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse malesuada aliquam lectus et mollis. Aliquam tincidunt diam a sapien pharetra ve-hicula.
Data Breach
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse malesuada aliquam lectus et mollis. Aliquam tincidunt diam a sapien pharetra ve-hicula.

Source: Several videos in this presentation from personal collection of Eugene Schultz, an unforgettable information security pioneer.

(Video Automatically Plays On This Slide)

Source: Several videos in this presentation from personal collection of Eugene Schultz, an unforgettable information security pioneer

2022-2027+

6. THE INTEGRATED BUSINESS RESILIENT CISO

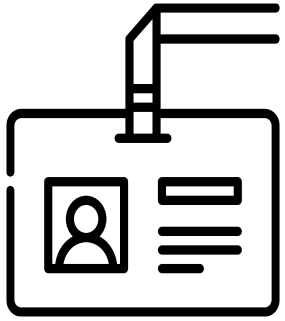
Tim Brown
CISO
SolarWinds

LUCKY?

UNLUCKY?

Tim Brown
CISO
SolarWinds

CISO EVOLUTION 1995-2027



1990s-2000

1 Security= Logon & Password FIRST CISO

2000-2004

2 Regulatory Compliance Era CISOs Hired

2004-2008

3 Risk-Oriented CISO Emerges

2008-2016

4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

2016-2022

5 The Privacy and Data-Aware CISO

2022-2027+

6 The Integrated Business Resilient CISO

Source: Adapted From T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications), New 6 Stage Model Updated in K. Engemann, J. Witty, Cybersecurity Risk Management (2024, De Gruyter)

2025 LEADING ORGANIZATION FUNCTIONS

Monitor

- Security Baseline Configuration Review
- Logging SIEM & Monitoring
- Vulnerability Assessment
- Managed Services
- Incident Response
- Forensic Analysis
- Threat Intelligence
- Security Analytics
- Insider Threat

Awareness

- End User Security Awareness
- Intranet Site and Policy Publication
- Targeted Awareness
- Phishing Programs
- Executive/Board Education and Advance Reporting

Risk

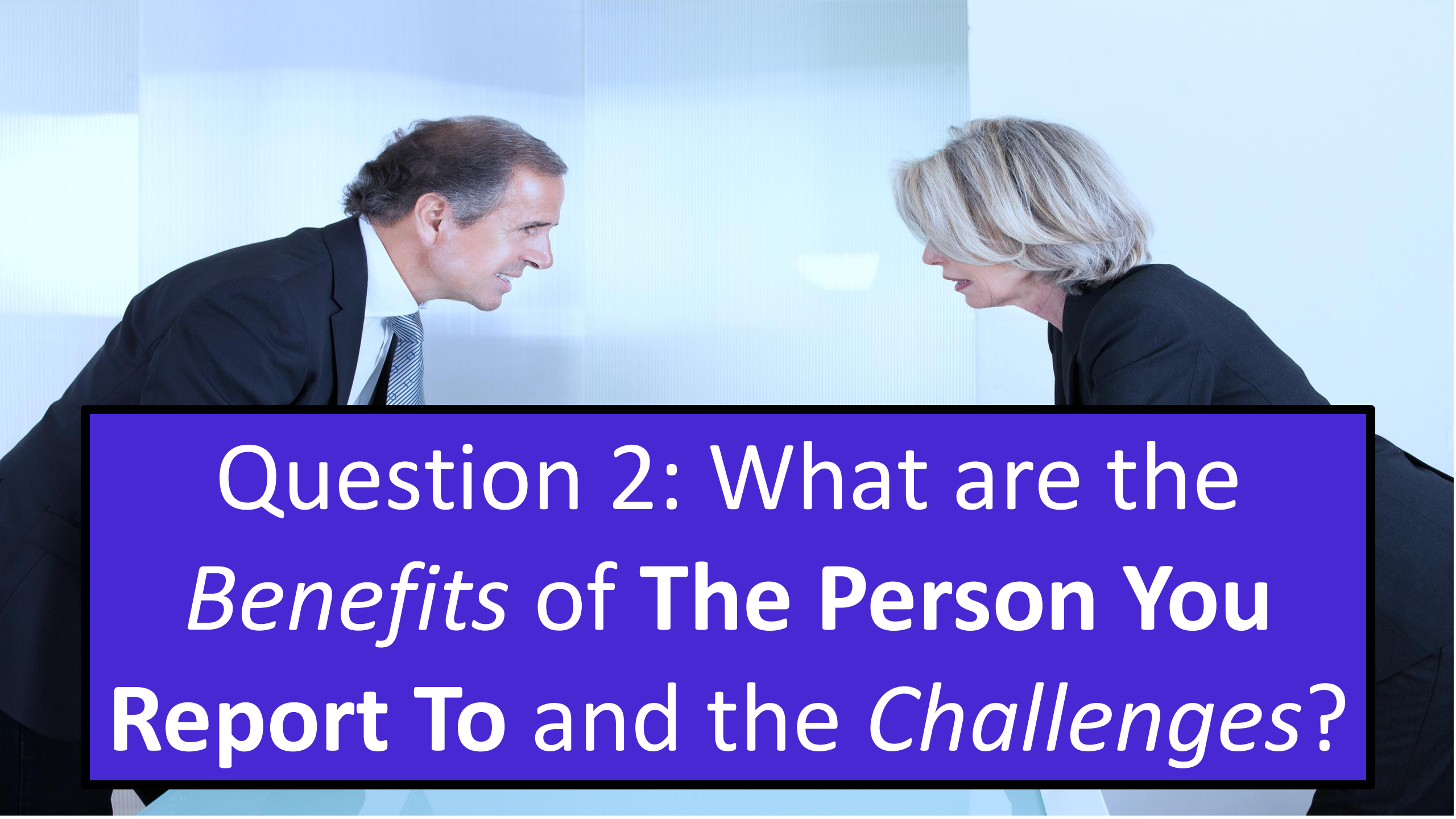
- Risk Assessment and Analysis
- Systems Security Plan
- Internal and External Penetration Testing
- Privacy
- Cyber Insurance
- 3rd Party Vendor Risk Management

Policy/Control

- Security Policy
- Security Architecture
- Security Control Assessment
- Identity Access Management
- Business Continuity & Disaster Recovery
- Control Framework Compliance
- Program Management

RSAC 2025 Conference

2. CISO Reporting Relationships PROS/CONS



Question 2: What are the *Benefits* of **The Person You Report To** and the *Challenges*?

LEGAL (GENERAL COUNSEL)

Anthem
National Government Services
United Government Services, LLC

Medicare
Security Officer

IT (CTO/CIO)

ZENECA syngenta

NA/Latin America
Security Manager

ManpowerGroup

Global CISO

Grant Thornton

Global CISO

INTERNAL AUDIT

Anthem
National Government Services
United Government Services, LLC

Medicare
Security Officer

RISK (CRO)

NORTHERN TRUST

CAO

Reporting to Information Technology (CIO)

- ❑ Familiarity with technical issues
- ❑ Easier access, stronger day-to-day relationship
- ❑ Informed on projects
- ❑ Member/Influencer of executive team

- ❑ Project deadlines are king
- ❑ Resource allocation issues, competing budgets
- ❑ Decisions are kept internal, limited visibility
- ❑ Security outsourcing combined with IT decisions

Reporting to Chief Legal Officer/General Counsel

- ❑ Emphasis on compliance, laws and ethics
- ❑ Documentation important
- ❑ Access to Legal Expertise
- ❑ Synergy with Chief Privacy Officer (CPO)

- ❑ Overly focused on compliance
- ❑ Lack of understanding of technical issues
- ❑ Underestimation of costs, resources, and level of effort to implement solutions

Reporting to Corporate/Physical Security

- ❑ Leverage law enforcement relationships
- ❑ Increased security incident communication
- ❑ Increased use of IT with CCTV

- ❑ May evoke “guns and guards” mentality
- ❑ Technical issue communication limited
- ❑ Difference in salary structures
- ❑ Skills and education very different

Reporting to Chief Operations Officer(COO)
Chief Administrative Officer (CAO)
Chief Human Resources Officer (CHRO)

- ❑ Demonstrates security is an enterprise-wide issue
- ❑ Closer relationship to CEO (one level away)
- ❑ Integration with business processes
- ❑ Communicates all forms of protection

- ❑ May not receive appropriate attentio
- ❑ Limited IT knowledge
- ❑ Short term focus on results

Reporting to CFO

- ❑ Supports controls compliance perspective
- ❑ Clout with top management
- ❑ Broad organizational view
- ❑ Has ear of the CEO

- ❑ Conflict of interest issues (Audit)
- ❑ Lack of IT knowledge
- ❑ Established adversarial relationships (IT audit) may carry over
- ❑ Revenue vs non-revenue producer

Reporting to CFO

“CFO was a peer to other executives and could apply influence laterally”

“CFO independence from technology operations leadership is better influence”

“CFO is a primary trusted advisor to the Board regarding risk, specifically cost-risk-benefit judgement”

“Reporting to CFO influences our cybersecurity budget and the resources we receive. This can be a positive and a negative”

-Survey of Chicago Area CISOs (2/2025, Fitzgerald)

Reporting to Risk Management (CRO)

- ❑ Risk advocate
- ❑ Focus on credit, operational and business risk
- ❑ Clout with board
- ❑ Familiarity with risk terminology

- ❑ Lack of business metrics
- ❑ Lack of appreciation for cybersecurity risk level
- ❑ Many organizations do not have the role

Reporting to CEO

- ❑ Raises cybersecurity visibility
- ❑ Tech companies prefer this model
- ❑ Short-term support
- ❑ Tech companies prefer model

- ❑ Lack of time for security issues
- ❑ Too many details for this level
- ❑ Revenue activities take precedent

RSAC 2025 Conference

3. Where the CISOs Report to Today – Surveys Say…

DISTANCE From CEO

PONEMON CISO STUDY: Only 22% of CISOs Report To CEO, 58% 1-2 Levels Away

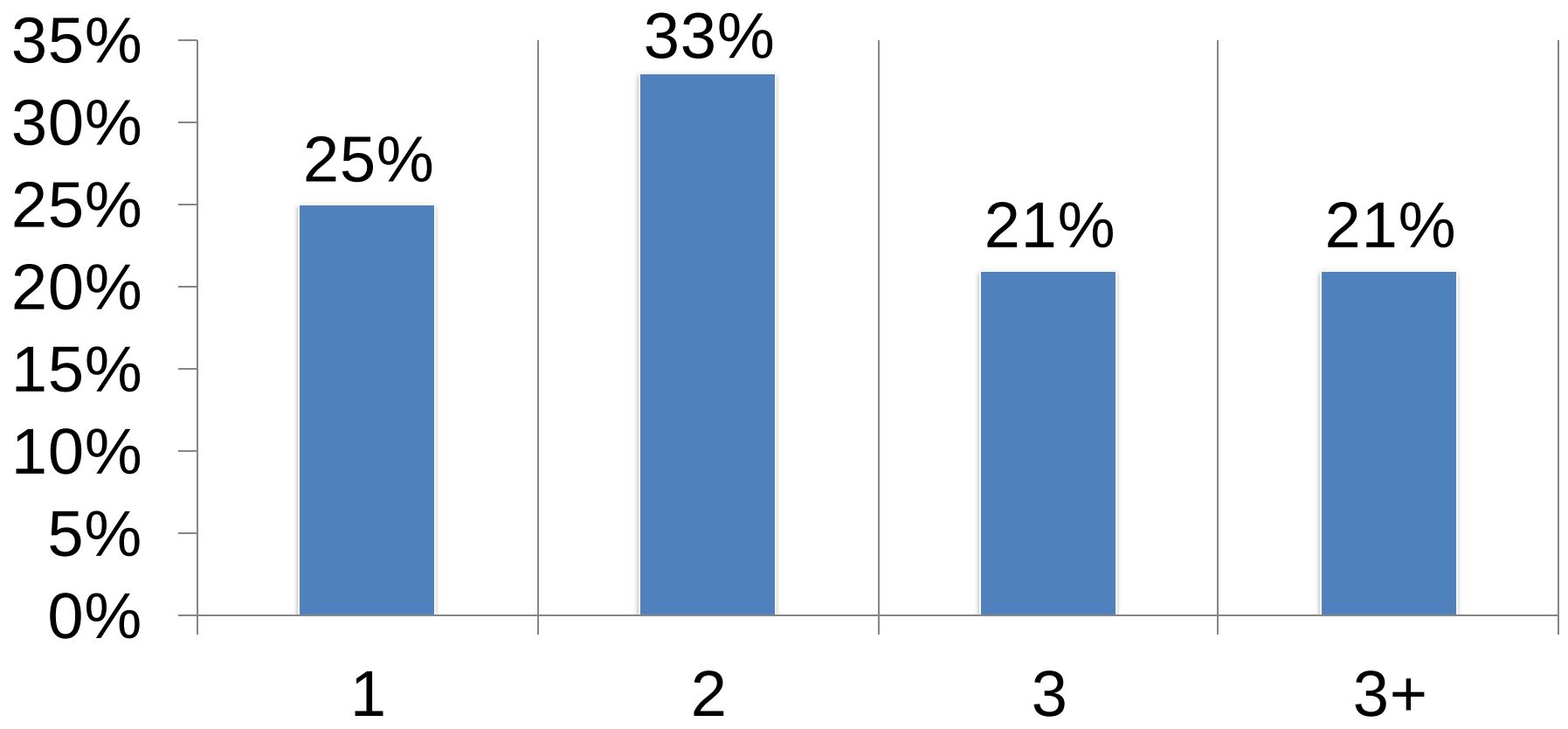


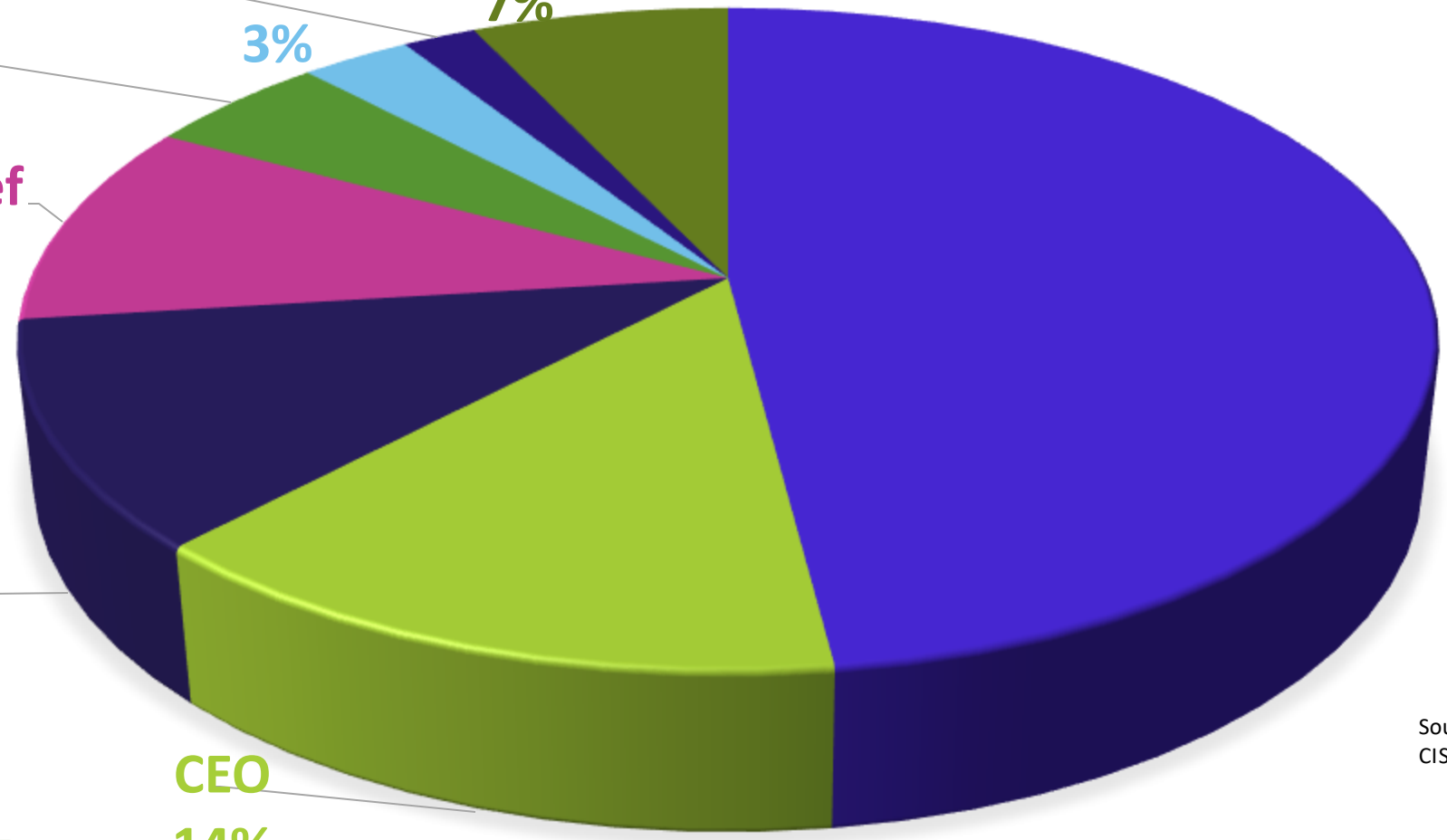
Figure 2. If you don't report to the CEO, how many levels are you away from the CEO?

Source: Ponemon Institute, The IT Cybersecurity Leader's Readiness to do the Job Today and in the Future, 4/2022

2025 IANS Study -CISO Reporting Level Depends On Organization Size and Title

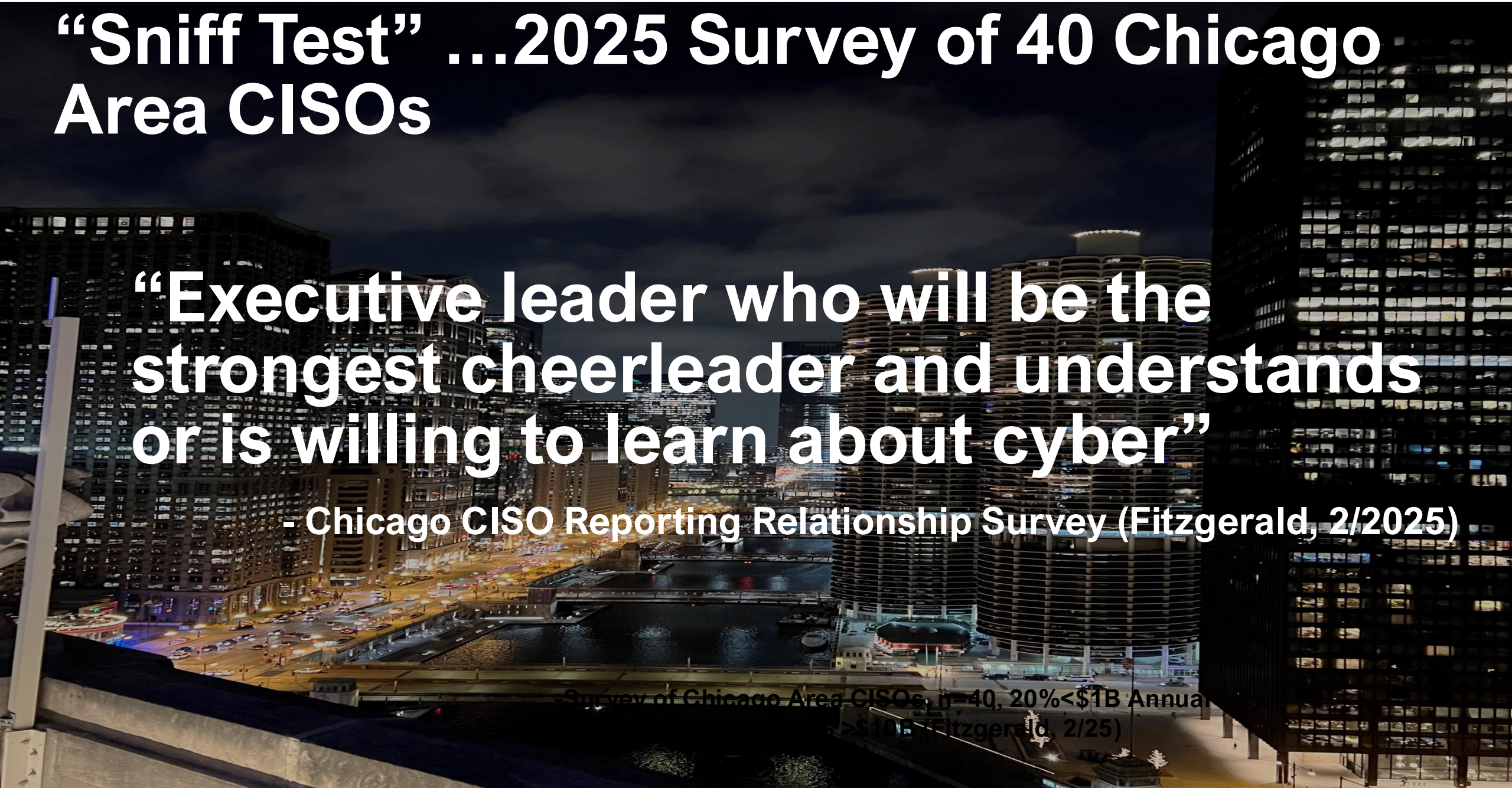
TO WHOM ARE CISOs REPORTING?

Heidrick & Struggles CISO Survey – 48% CISOs Reporting to IT



Source: Heidrick & Struggles Global CISO Survey 2024, n=408

“Sniff Test” …2025 Survey of 40 Chicago Area CISOs

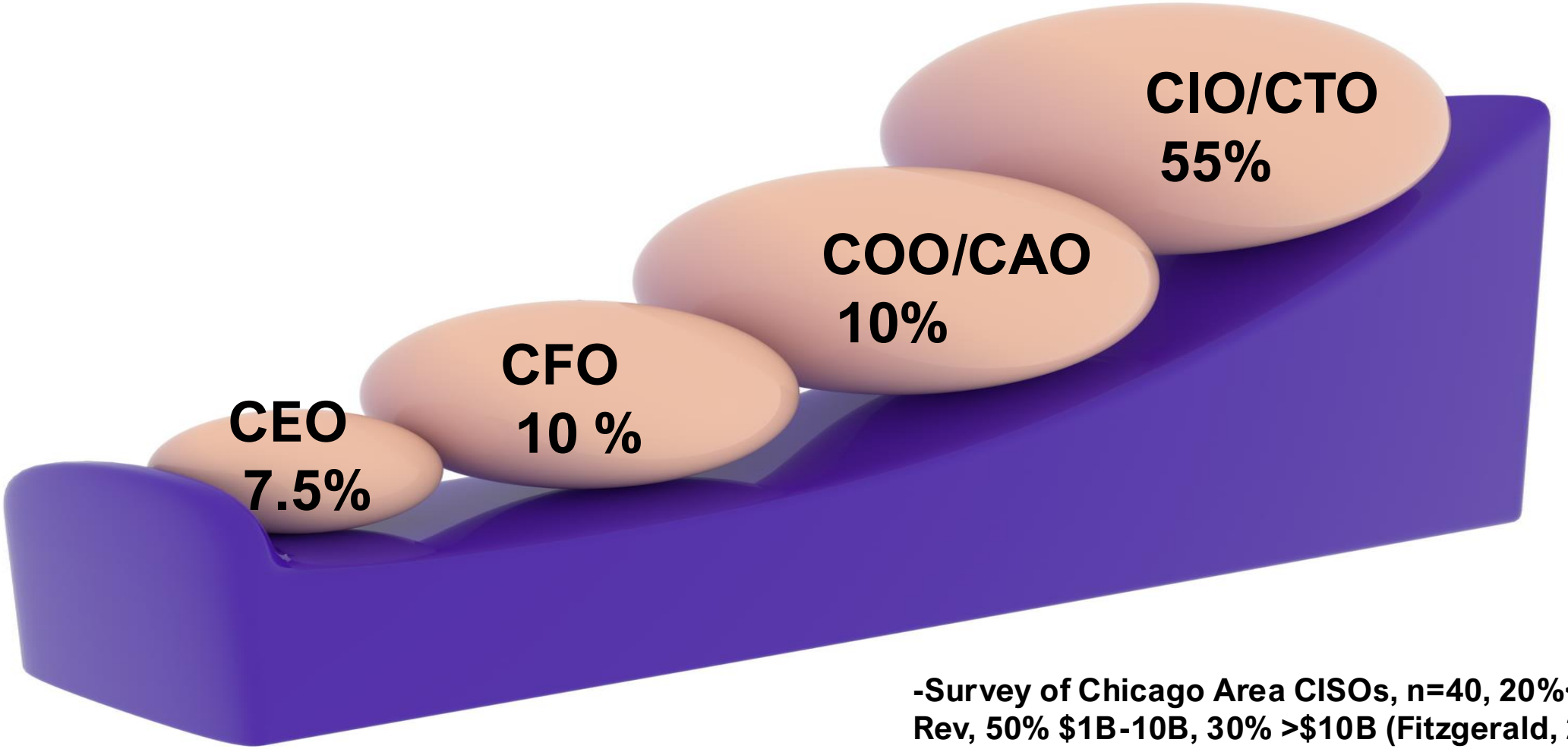


“Executive leader who will be the strongest cheerleader and understands or is willing to learn about cyber”

- Chicago CISO Reporting Relationship Survey (Fitzgerald, 2/2025)

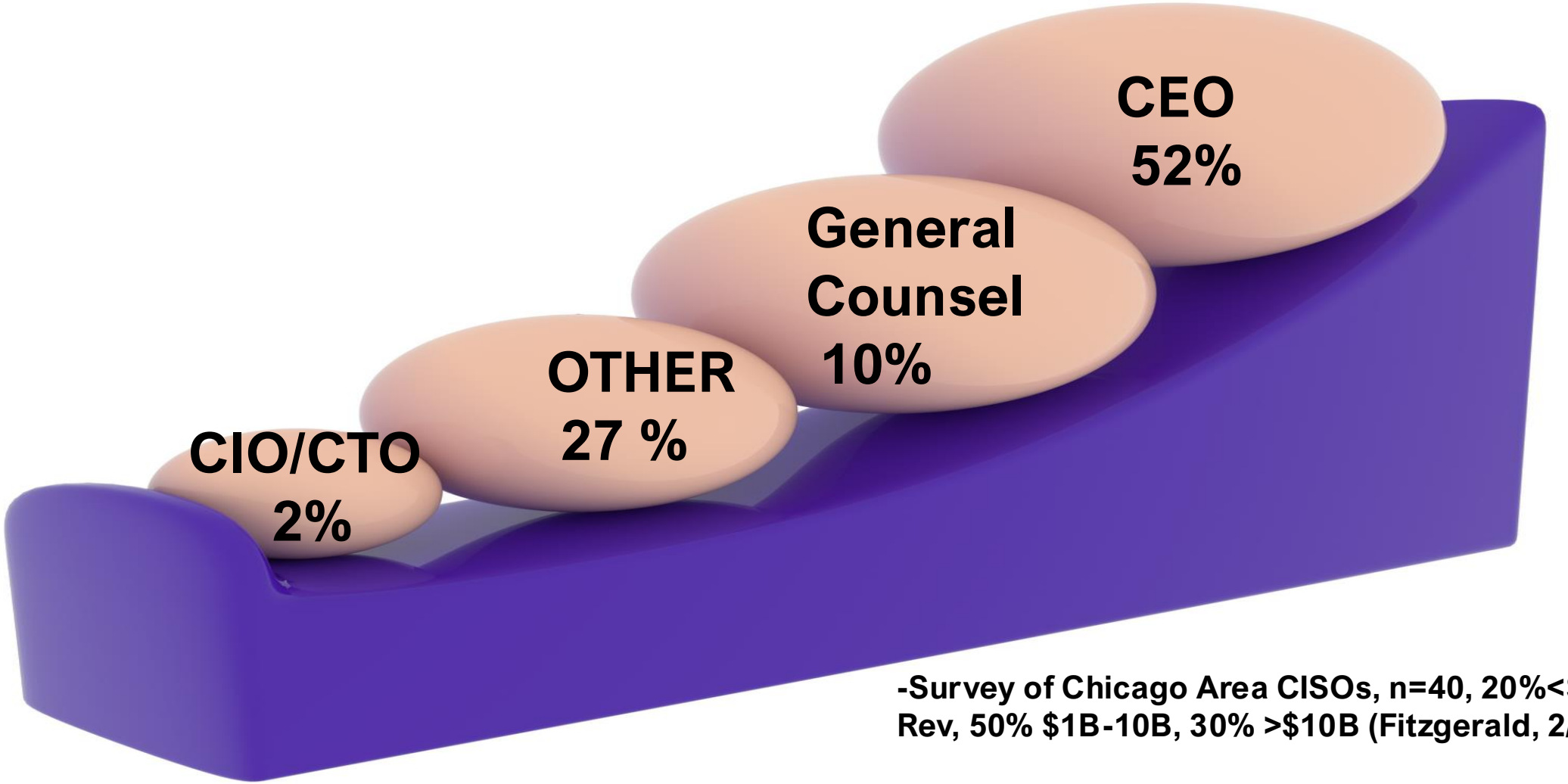
Survey of Chicago Area CISOs, n=40, 20%<$1B Annual
>$10B (Fitzgerald, 2/25)

Q1: Who Do You Currently Report To?

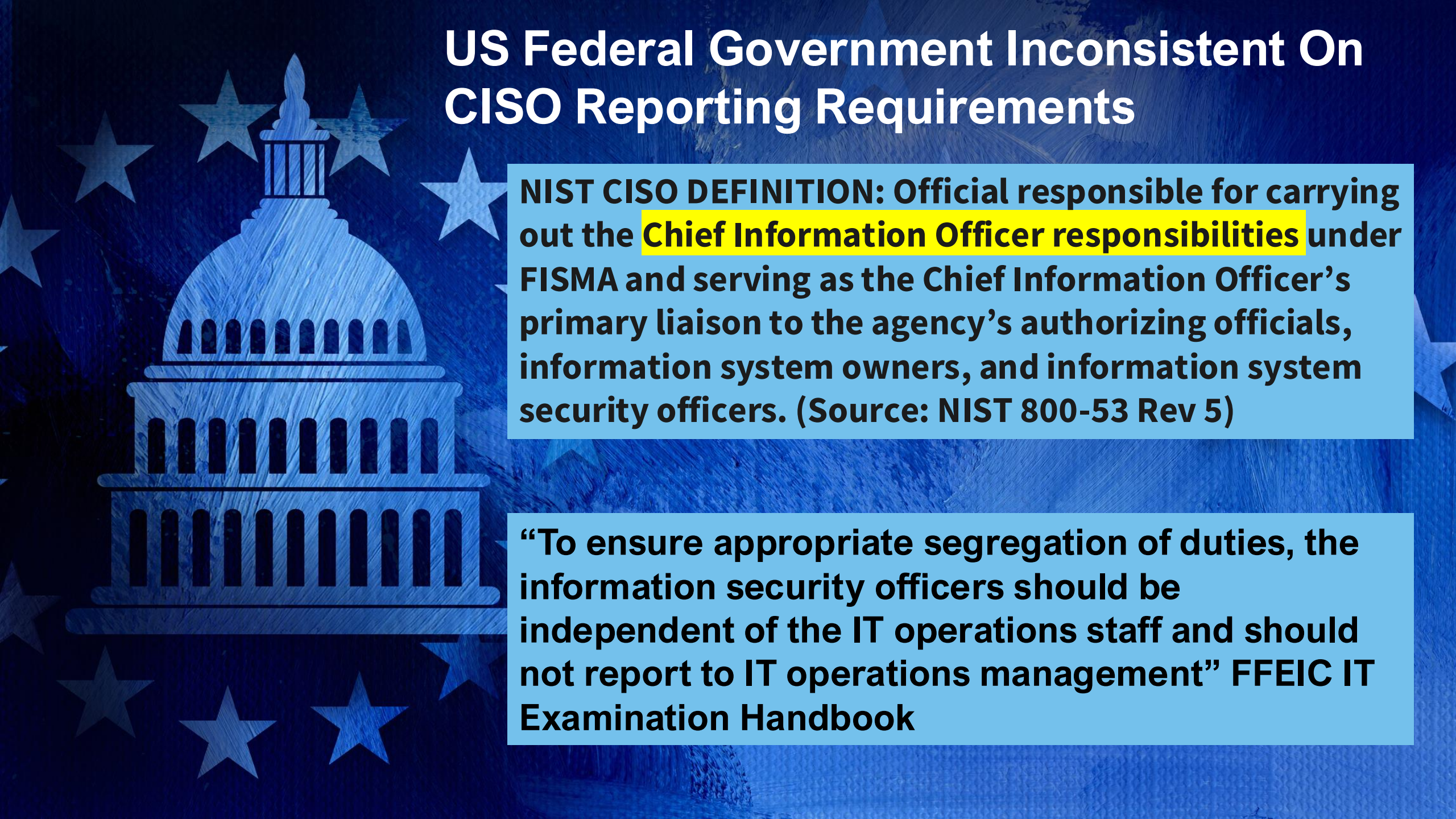


-Survey of Chicago Area CISOs, n=40, 20%<$1B Annual Rev, 50% $1B-10B, 30% >$10B (Fitzgerald, 2/25)

Q2: Who do you believe the CISO should really report to for maximum effectiveness?



-Survey of Chicago Area CISOs, n=40, 20%<$1B Annual Rev, 50% $1B-10B, 30% >$10B (Fitzgerald, 2/25)

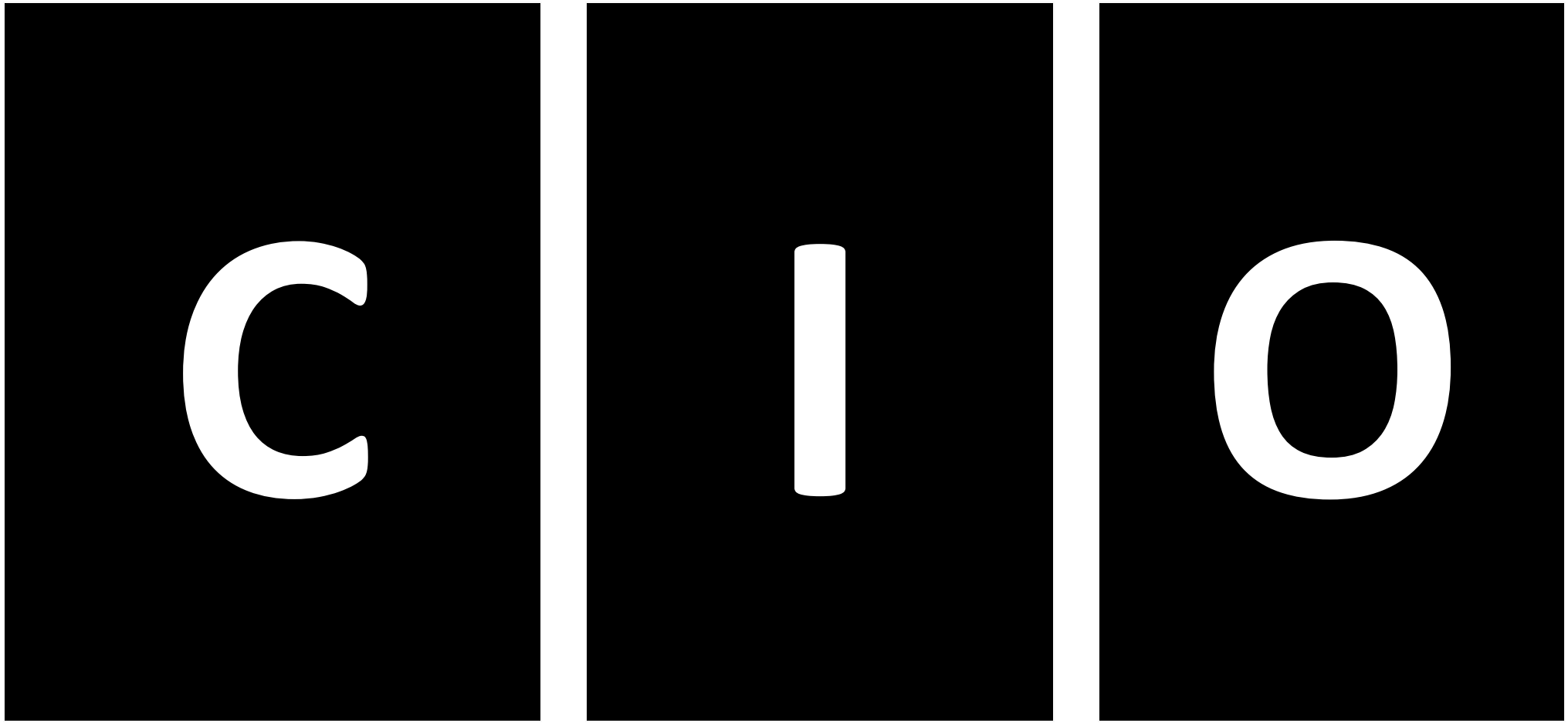


US Federal Government Inconsistent On CISO Reporting Requirements

NIST CISO DEFINITION: Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. (Source: NIST 800-53 Rev 5)

"To ensure appropriate segregation of duties, the information security officers should be independent of the IT operations staff and should not report to IT operations management" FFEIC IT Examination Handbook

And While Changing, Most CISOs Still Report To . . .

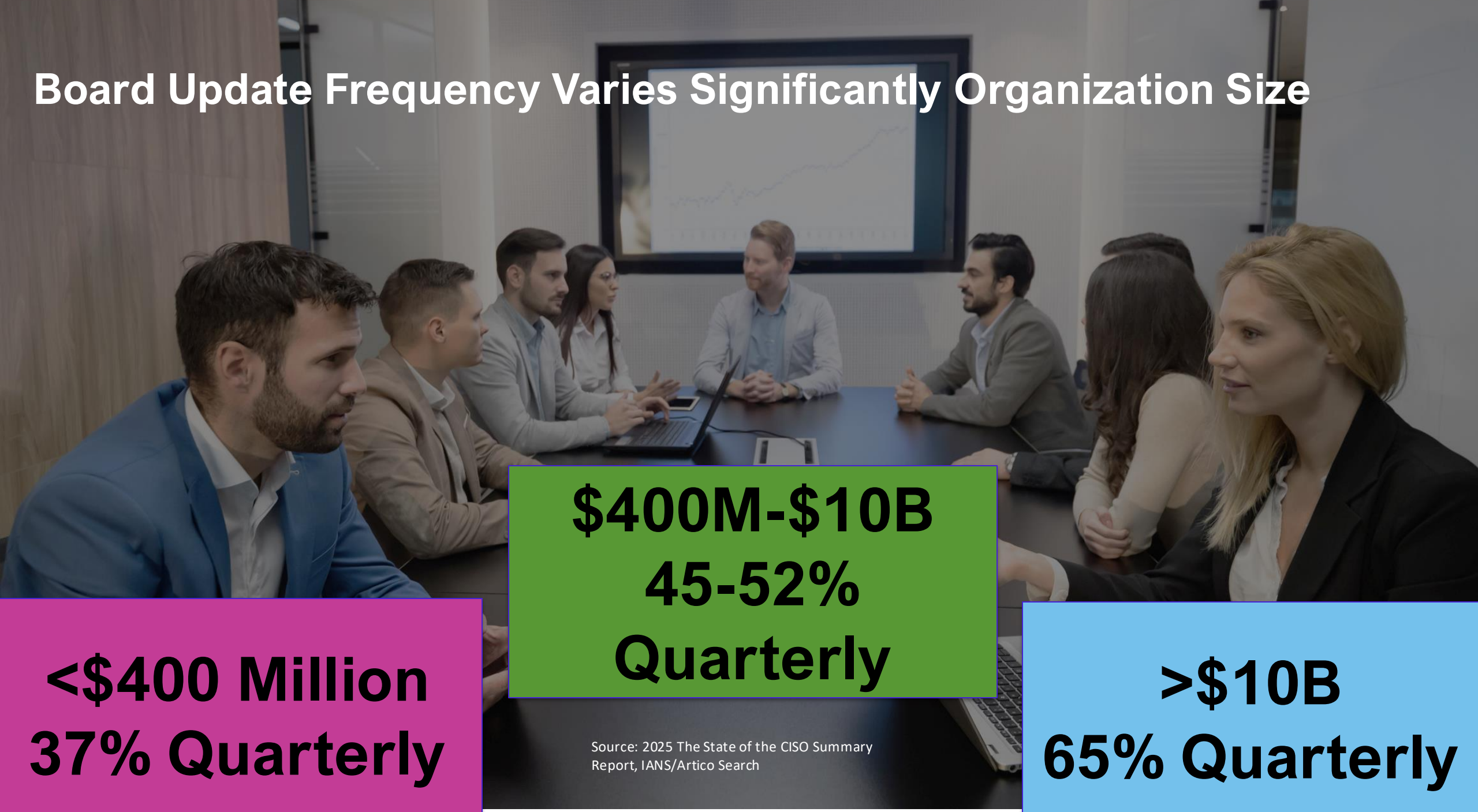


RSAC 2025 Conference

4. Board Reporting/Final Thoughts

Cybersecurity Tone at the Top can only be supportive if you are listening to the Tone at the Bottom.

Board Update Frequency Varies Significantly Organization Size



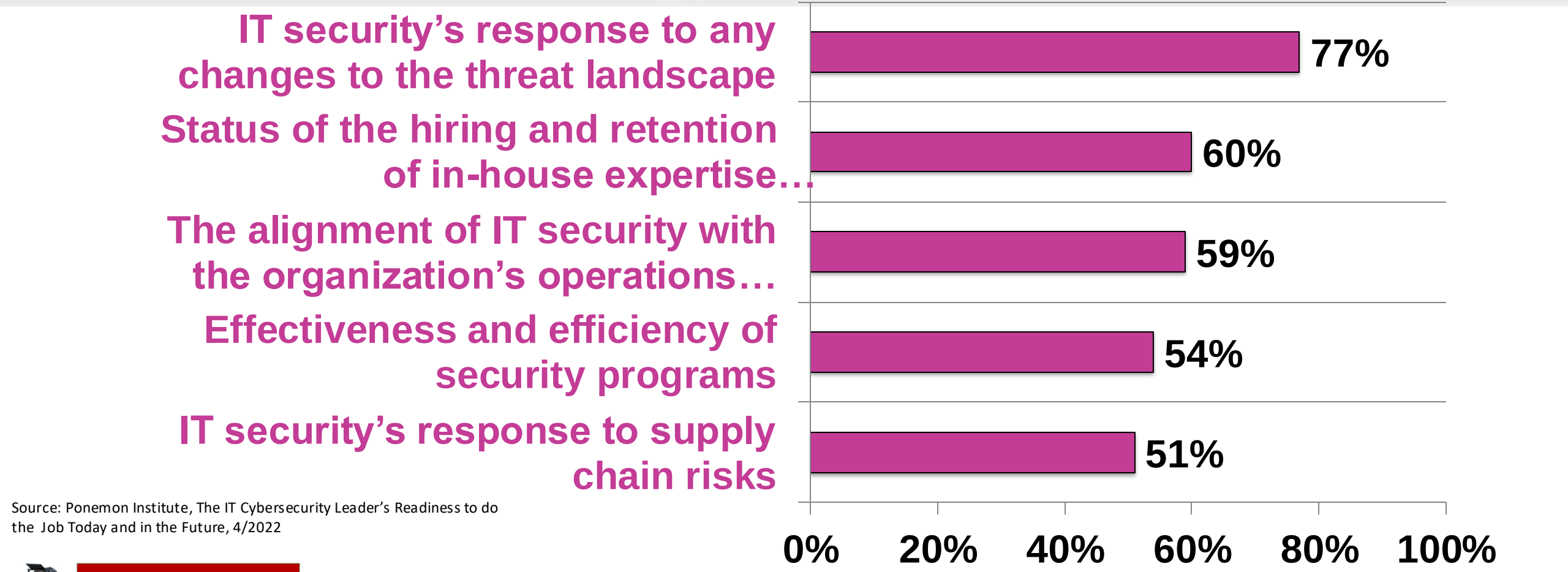
<$400 Million
37% Quarterly

$400M-$10B
45-52%
Quarterly

>$10B
65% Quarterly

Source: 2025 The State of the CISO Summary Report, IANS/Artico Search

CISO Reporting Relationship With The Board… Top 5 Topics



Source: Ponemon Institute, The IT Cybersecurity Leader's Readiness to do the Job Today and in the Future, 4/2022

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

RSAC 2025 Conference

Today We Covered…

- CISO Evolution and Different CISO Types
- Reporting Relationships PROS/CONS
- CISO Reporting Surveys
- Board Reporting Considerations

Apply What You Have Learned Today

- Next week you should:
  - Determine Your Organization's and CISO Type
- In the first three months following this presentation you should:
  - Review pros/cons specific to your current reporting structure
  - Determine where the CISO role would be most effective
- Within six months you should:
  - Solicit input From business peers on the best reporting relationship
  - Initiate moves within organization to appropriately position the CISO and Team

Before Jumping Ship, Understand Your Focus Area, Your Own CISO Reporting Relationship Pros and Cons, And How You Can...

ADAPT

THANK YOU FOR YOUR TIME!

QUESTIONS?

BOOK SIGNING AT RSAC BOOKSTORE IN SOUTH MASCONE MEZZANINE
TUESDAY APRIL 29
11:30AM

Todd Fitzgerald
CISO SPOTLIGHT, LLC
www.linkedin.com/in/toddfitzgerald
www.cisospotlight.com

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

Resources For Cybersecurity Leaders & Teams

#1 BEST SELLER 2019-2024 – 6 YEARS!

CANON CYBERSECURITY HALL OF FAME WINNER

RSAC 2025 Conference

RSAC | 2025 Conference

Many Voices.
One Community.

For More Information:

Contact Todd Fitzgerald

tfitzgerald@cisospotlight.com

www.amazon.com/author/toddfitzgerald

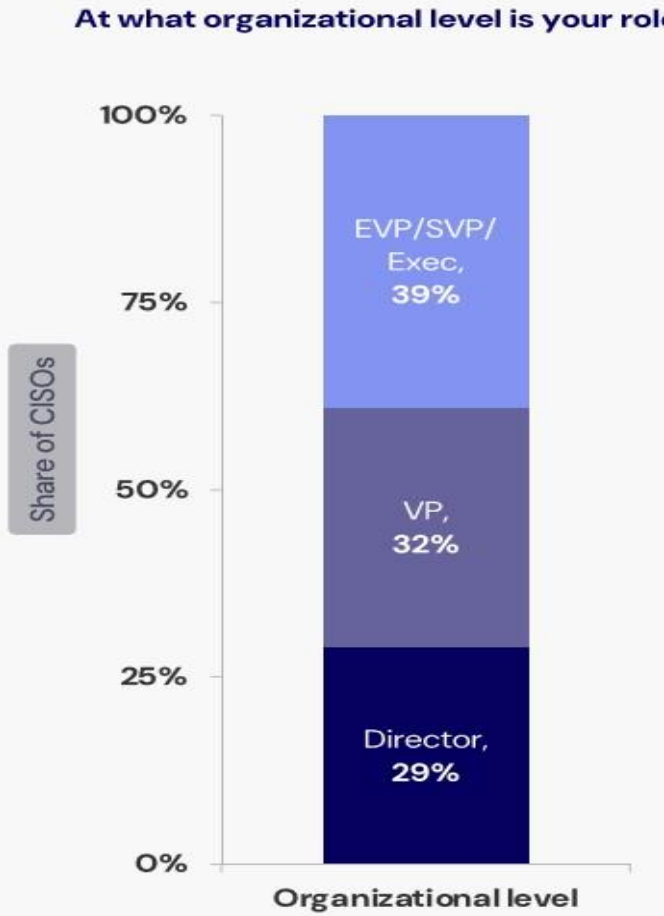
RSAC 2025 Conference

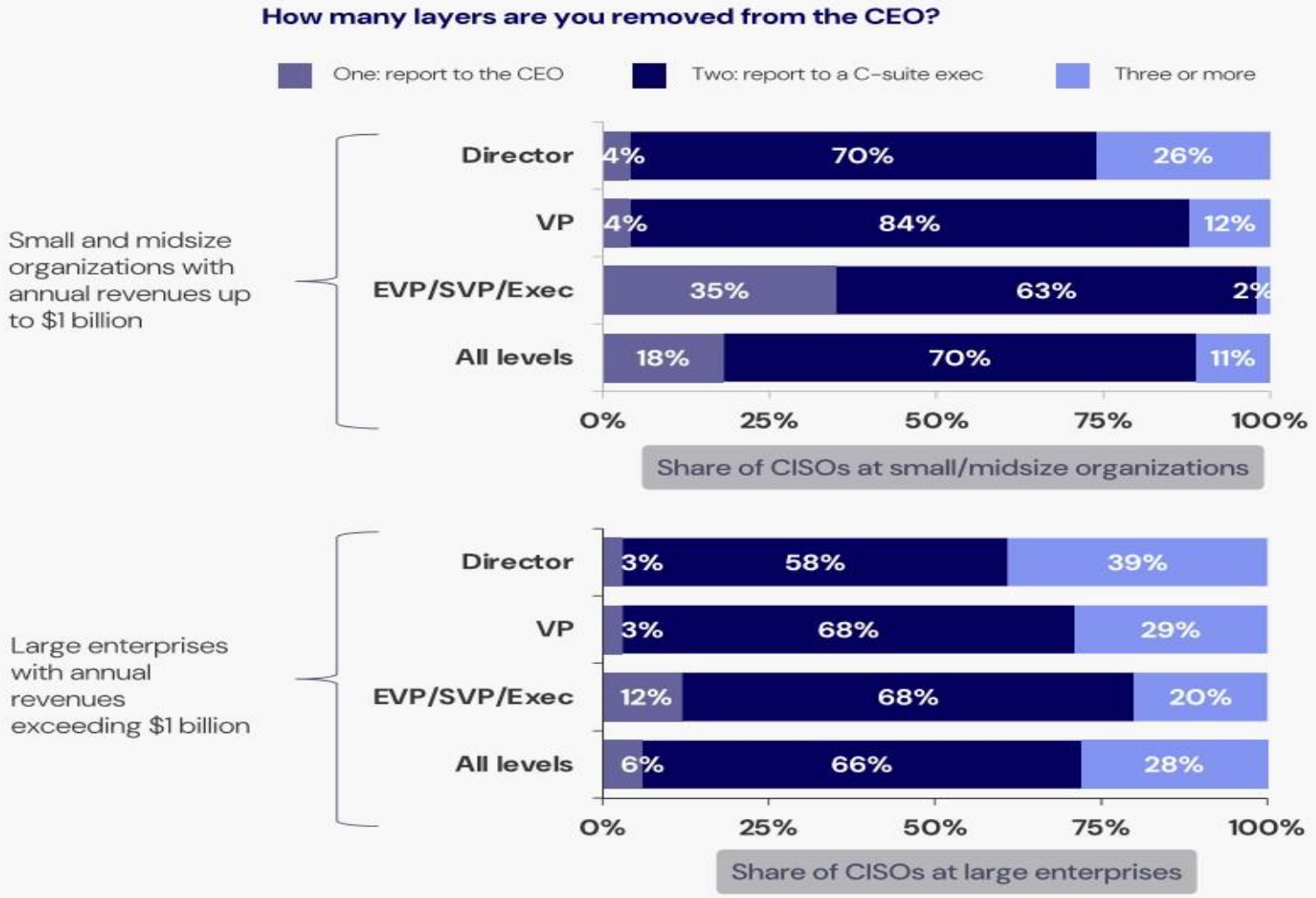
APPENDIX

Detailed Slides Supporting Presentation

Many Voices.
One Community.

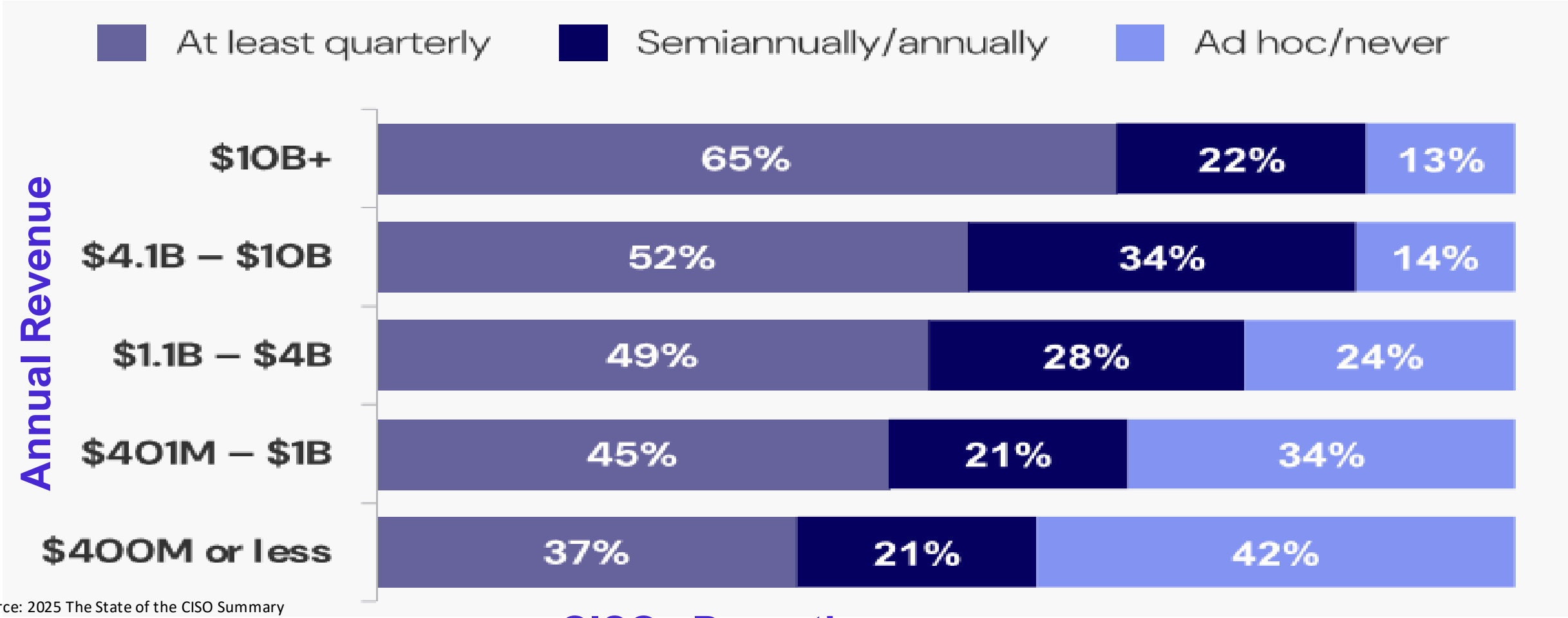
Most CISOs Are VP Level or Higher, With Close Proximity to C-Suite




How many layers are you removed from the CEO?
One: report to the CEO
Two: report to a C-suite exec
Three or more
Small and midsize organizations with annual revenues up to $1 billion
Director 4% 70% 26%
VP 4% 84% 12%
EVP/SVP/Exec 35% 63% 2%
All levels 18% 70% 11%
0% 25% 50% 75% 100%
Share of CISOs at small/midsize organizations
Large enterprises with annual revenues exceeding $1 billion
Director 3% 58% 39%
VP 3% 68% 29%
EVP/SVP/Exec 12% 68% 20%
All levels 6% 66% 28%
0% 25% 50% 75% 100%
Share of CISOs at large enterprises

Source: 2025 The State of the CISO Summary Report, IANS/Artico Search

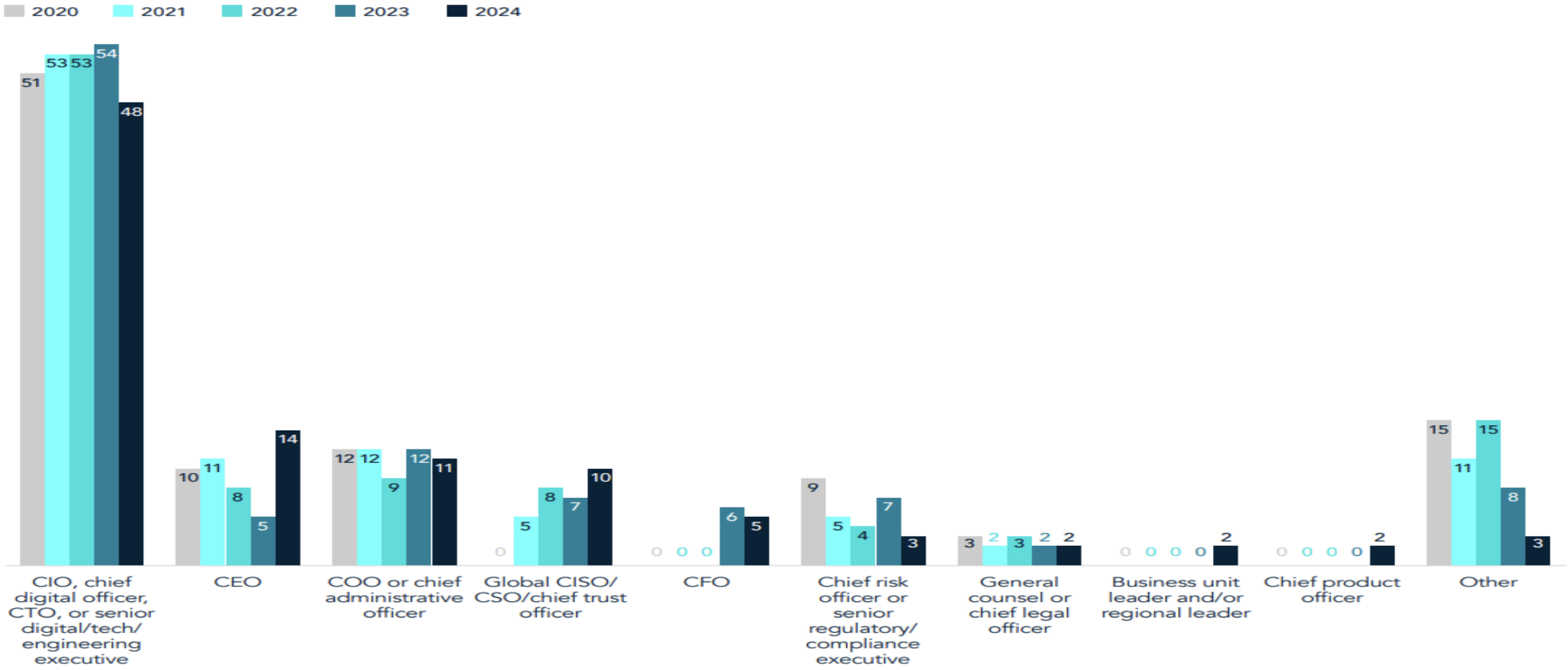
Board Update Frequency Varies Significantly by Size of the Organization



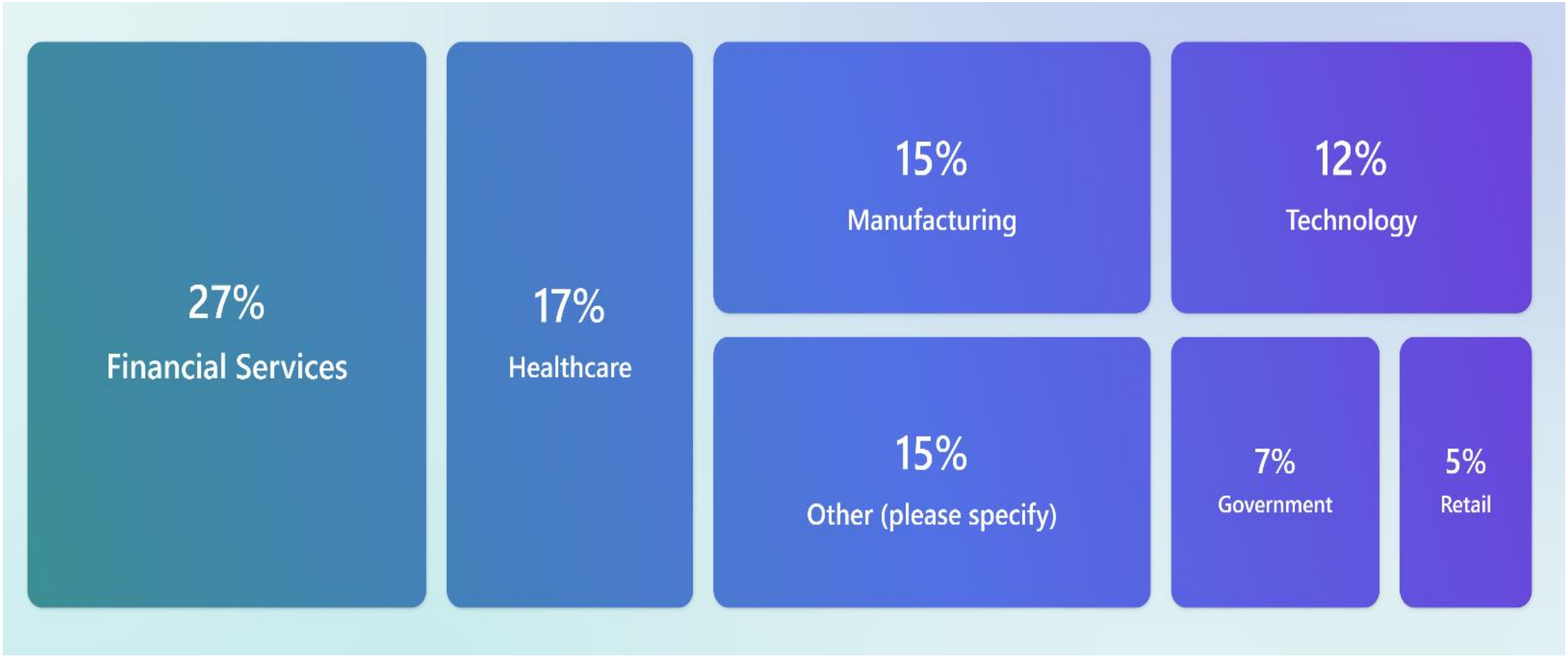
Source: 2025 The State of the CISO Summary Report, IANS/Artico Search

CISOs Reporting

Role Reporting Has Not Changed Significantly Over Past 5 Years (2020-2024)

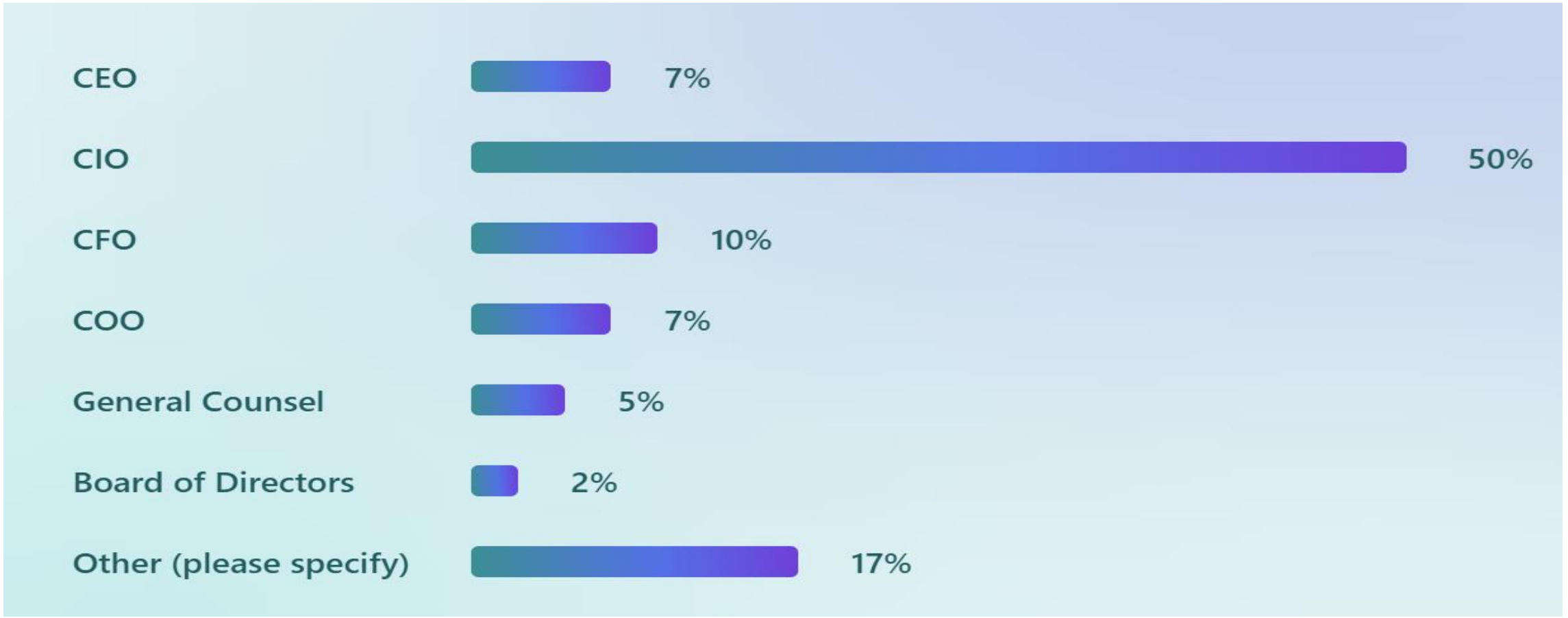

2020
2021
2022
2023
2024
51 53 53 54 48
10 11 8 5 14
12 12 9 12 11
0 5 8 7 10
0 0 0 6 5
9 5 4 7 3
3 2 3 2 2
0 0 0 0 2
0 0 0 0 2
15 11 15 8 3
CIO, chief digital officer, CTO, or senior digital/tech/ engineering executive
CEO
COO or chief administrative officer
Global CISO/ CSO/chief trust officer
CFO
Chief risk officer or senior regulatory/ compliance executive
General counsel or chief legal officer
Business unit leader and/or regional leader
Chief product officer
Other

What Industry Does Your Organization Belong To?



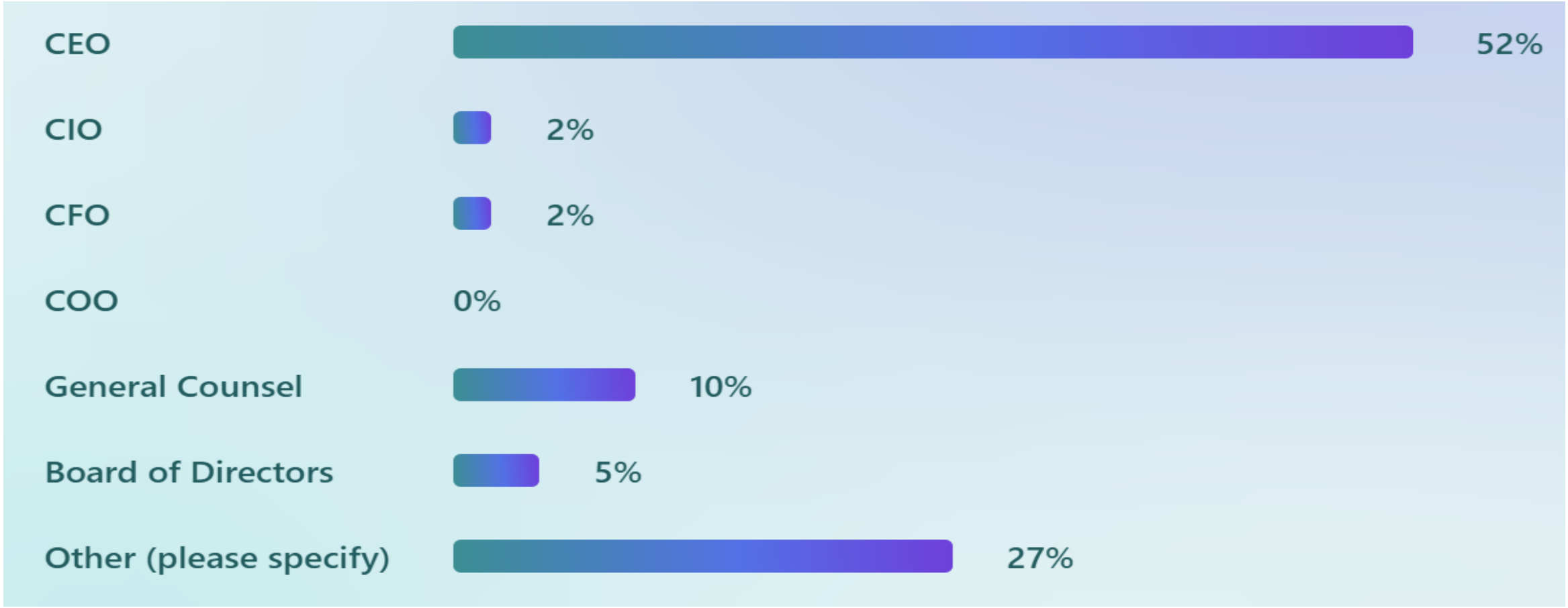
-Survey of Chicago Area CISOs, n=40, 20%<$1B Annual Rev, 50% $1B-10B, 30% >$10B (Fitzgerald, 2/25)

Who Do You Currently Report To?



-Survey of Chicago Area CISOs, n=40, 20%<$1B Annual Rev, 50% $1B-10B, 30% >$10B (Fitzgerald, 2/25)

Q: Who do you believe the CISO should really report to for maximum effectiveness?



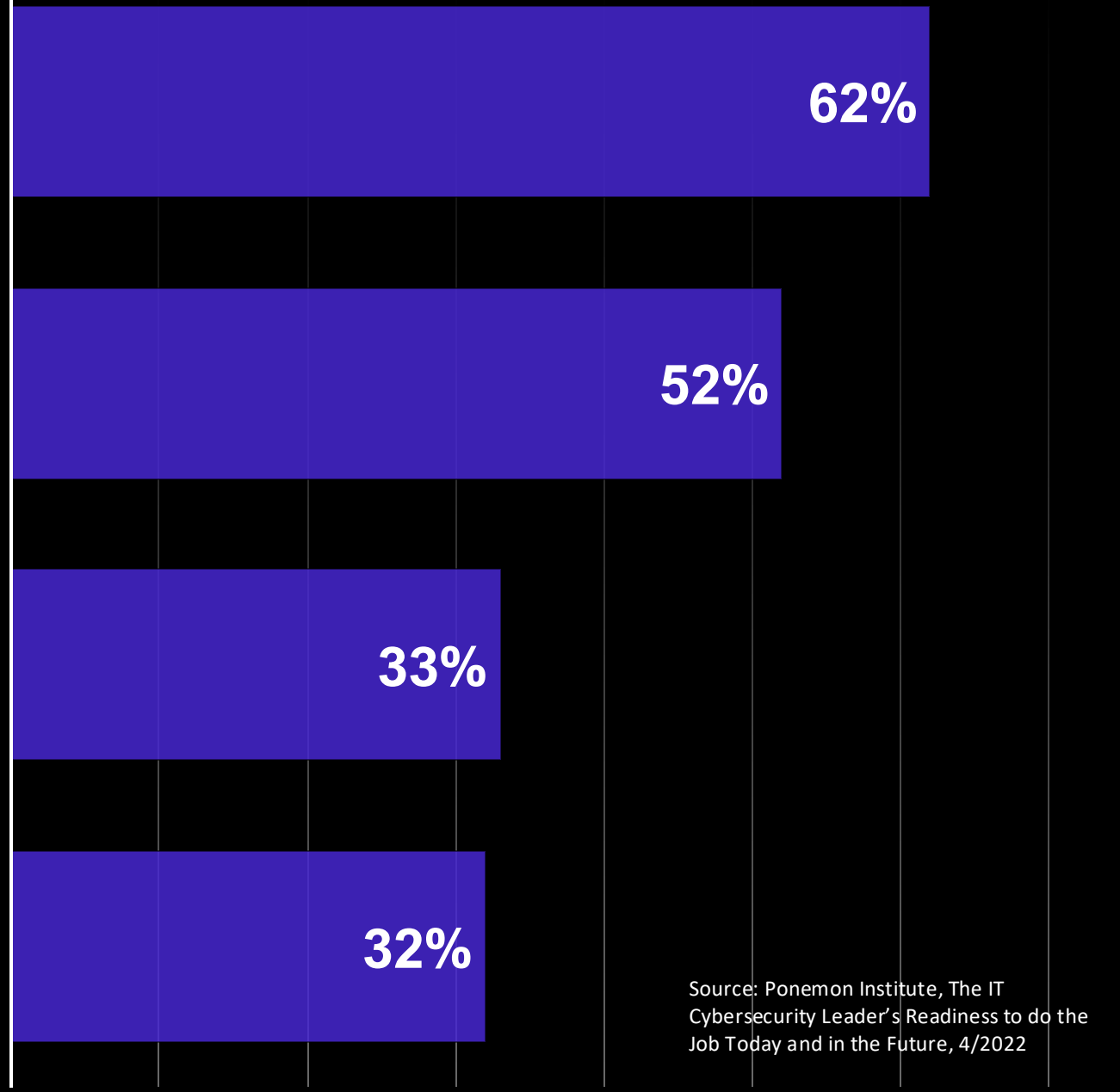
-Survey of Chicago Area CISOs, n=40, 20%<$1B Annual Rev, 50% $1B-10B, 30% >$10B (Fitzgerald, 2/25)

IT IS A CHALLENGE TO INCREASE THE VISIBILITY AND IMPORTANCE OF CYBERSECURITY

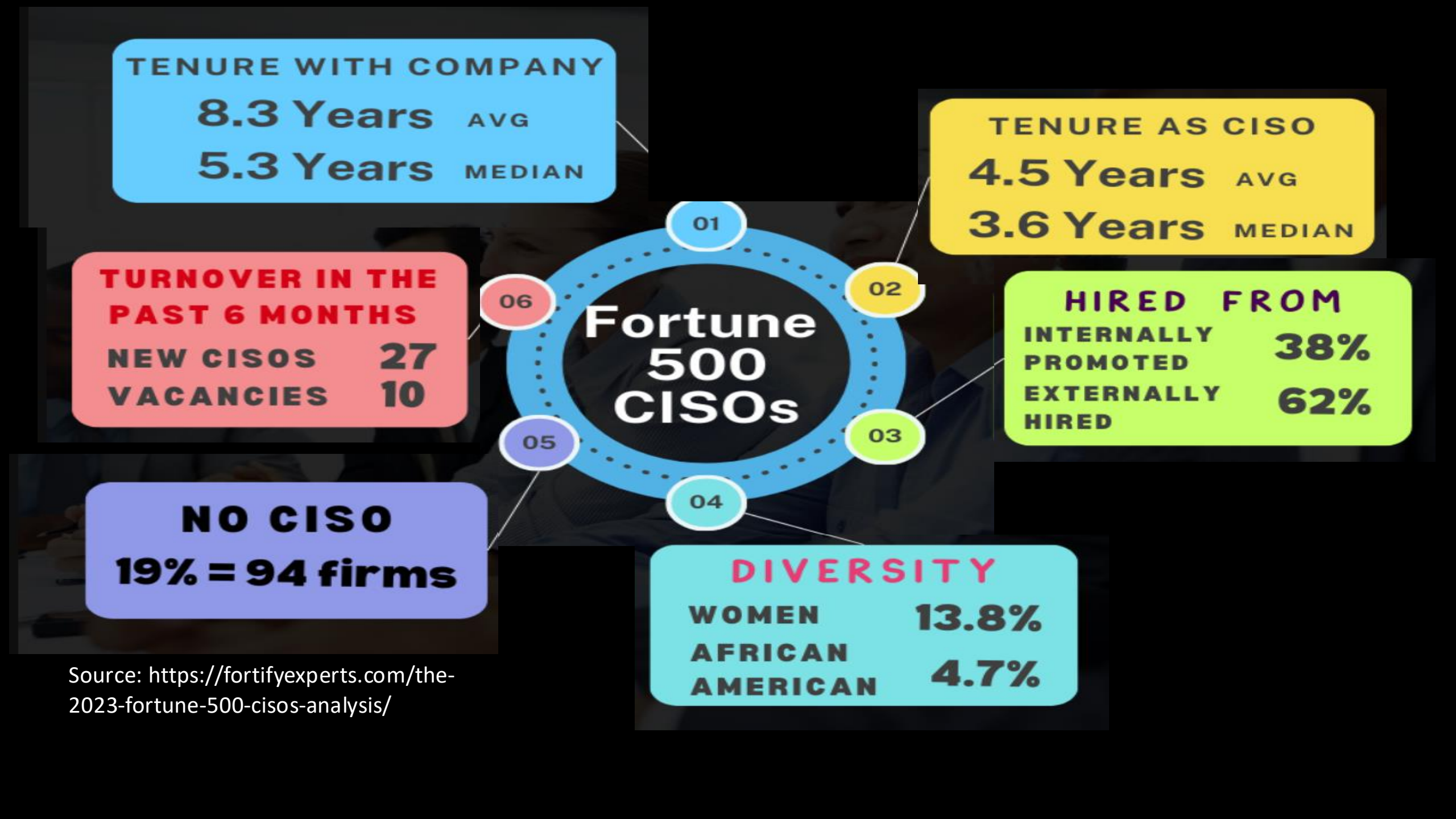
A STRONG CYBERSECURITY POSTURE MAY BE SACRIFICED FOR WHAT MAKES THE CIO AND IT DEPARTMENT APPEAR SUCCESSFUL IN COMPLETING THEIR PROJECTS ON TIME AND MAINTAINING THE ORIGINAL BUDGET

CYBERSECURITY IS A RELATIVELY IMMATURE FUNCTION AND THEREFORE IS NOT WELL-FUNDED OR UNDERSTOOD

CYBERSECURITY IS STILL SEEN AS AN IT ISSUE THAT IS BEST UNDERSTOOD AND MANAGED BY THE FUNCTION RESPONSIBLE FOR THE ORGANIZATION'S INFORMATION SYSTEMS



Source: Ponemon Institute, The IT Cybersecurity Leader's Readiness to do the Job Today and in the Future, 4/2022



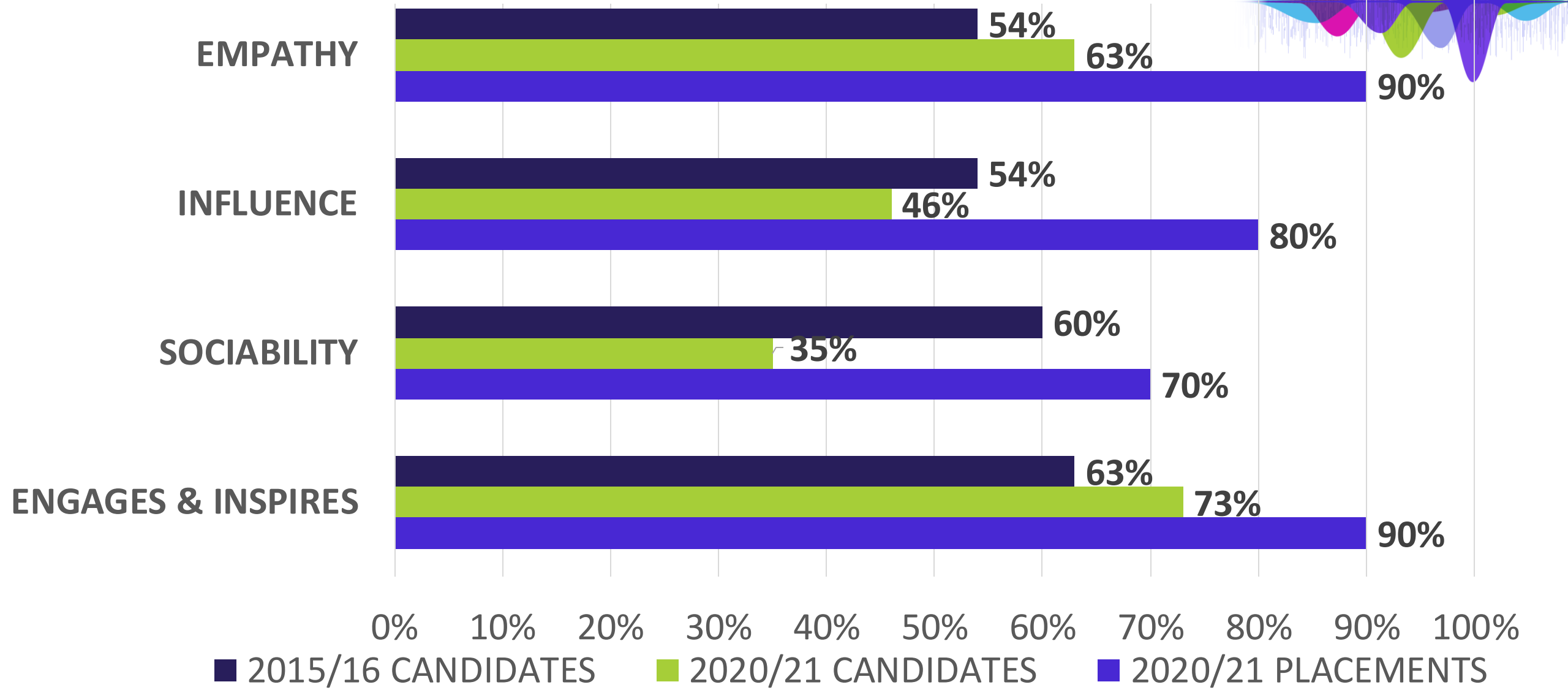
Source: https://fortifyexperts.com/the-2023-fortune-500-cisos-analysis/

What Degrees Do Fortune 500 CISOs Prefer ?

UNDERGRADUATE	GRADUATE
Computer Science 18.4%	MBA 44.8%
Business 9.2%	Computer Science 7.7%
Management Information Systems 8.9%	Management Information Systems 5.0%

Source: Forrester Research, Base 326 Fortune 500 CISOs reporting undergraduate education on LinkedIn; 181 Fortune 500 CISOs reporting graduate degrees

CISO Skills Expectations Changing



Source: Korn Ferry, Meet the New CISOs, 2021

To Be Effective, the CISO Must Skill Up

- Talking vs Listening
- Influencing/Negotiating
- Written Communication
- Networking
- Executive Presence
- Business Terminology/Processes
- Certification
- Presentation
- Budgeting/Financial Skills
- Technical Excellence
- Team Dynamics